Online Safety Policy

Date completed: **September 2026**

Completed by: **Samantha Wilson**

Review: **Annually, or unless when guidance updates**

Policy Development & Consultation

Ladywood staff have contributed to the development of this policy during staff and curriculum meetings, and have been consulted throughout the process.

Background Information about the School

Ladywood School is an Outstanding Special School situated in Bolton. It caters for primary aged pupils with complex learning difficulties and pupils with a diagnosis of Autistic Spectrum Disorder.

At Ladywood we aim to provide all our pupils with a broad and relevant education. We do this is in a positive environment that reflects our commitment to high expectations for all.

At Ladywood, our pupils are given the very best care and support to ensure that they gain essential skills and receive the very best from their educational experiences. Our team work in close partnership with our parents and the wider professional community to ensure a holistic and dynamic network of support for all pupils. Our curriculum is designed with pupils' individual strengths and needs at the heart of their learning. Every step is taken to ensure that our pupils develop a love of learning, in an engaging, challenging and creative environment.

Philosophy

This document is a statement of the aims, principles and strategies for Online Safety at Ladywood School.

The policy has been developed to give a clear view of how technology in the curriculum should encourage pupils to acquire and develop essential Computing skills for learning and life by providing each child with broad, balanced, relevant experiences whilst safeguarding our pupils in the digital environment. "Online safety" is a core part of safeguarding. It encompasses child protection, behaviour, wellbeing, inclusion, staff conduct, data security, use of technology, and safe use of AI.
We aim to ensure all pupils use technology and online resources in a way that is safe, responsible, respectful, and appropriate to their age, understanding and needs.

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of parents/carers/ staff

Scope of the Policy

The regulation and use of technical solutions to safeguard pupils are important and must be balanced with teaching the necessary skills to enable pupils to take responsibility for their own safety in an ever-changing digital world.
The National Computing Curriculum states that pupils should be able to use technology safely, respectfully and responsibly keeping personal information private, recognise acceptable or unacceptable behaviour and identify a range of ways to report concerns about content and contact. Pupil's safety is paramount and they will receive the help, guidance and support through the whole curriculum to enable them to recognise and avoid online risks and to build their resilience. During the delivery of the curriculum staff will reinforce and consolidate safe online learning This policy applies to all members of the school community who have access to and are users of school ICT systems and online resources, both in and out of school. The school will deal with incidents as outlined within this policy, within the remit of their safeguarding, behaviour and anti-bulling policies (and others when applicable).
This policy applies to all pupils, staff, governors, visitors, volunteers, external providers, and contractors using the school's systems or connecting personal devices on site.

Development of the Policy

This Policy has been reviewed and ratified by the school's own relevant parties* i.e.

· Head teacher

· Local Governing Body (designated Safeguarding Governor Lead)

· Designated Safeguarding lead (DSL)

· Computing lead / team

Legislative & Policy Context

The following legislation to inform our policy:

- *Keeping Pupils Safe in Education 2026* (England). The Key Leaders+2EdTech Innovation Hub+2
- UK GDPR, Data Protection Act, Online Safety Act 2023, safeguarding law, SEND Code of Practice, etc.
- DfE's **Generative AI: product safety expectations** for schools. EdTech Innovation Hub+2Education Experts+2
- Filtering and monitoring standards as required by DfE and Ofcom, including annual review. SWGfL+2Education Experts+2

Schedule of Monitoring and Review

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, safeguarding updates, new online threats or incidents that have taken place.

The implementation of this Online Safety Policy will be monitored by the:

- Head teacher
- Trustees/ Governing board
- DSL
- Computing Lead / team

The school will monitor the impact of the policy using:

- Identify pupils at greater risk of harm.
- Regular Audits of pupils and families' online behaviour and harms for baseline, this information to feed into risk assessment.
- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited) Internal monitoring data for network activity
- Filtering and Monitoring alert system.

Should serious online incidents take place, including Filtering and Monitoring actions, the following external persons / agencies should be informed: Head teacher, School DSL, LADO, Police See Appendix 1

Roles and Responsibilities

Headteacher:
Ensure staff understand policy; ensure systems and practices are safe; ensure DSL has sufficient training and resources.

Governors:
Ensure policies (including online safety and AI) are up to date, compliant, adequately resourced, and that there is oversight of implementation. Receive reports on filtering/monitoring, risk assessments, incidents.
Governors are responsible for the approval of this Online Safety Policy and for reviewing its effectiveness. This will be carried out by the Governing board, receiving regular information about online incidents and monitoring reports.

Designated Safeguarding Lead (DSL)
Take lead for online safety and AI risks; monitor trends in online harms (including AI generated); support and deliver staff training; ensure incidents are recorded and escalated appropriately; liaise with external agencies.

DSL takes the lead role in managing online safety, ensuring that school has clear procedures to address any safeguarding concerns and uphold the school's prevent duty obligations.

The DSL will review and update the school's Filtering and Monitoring procedures, clearly defining roles and responsibilities within these processes. When assessing filtering and monitoring systems, governing bodies and relevant parties will consider the number of pupils at risk and the proportionality of costs versus safety risks.

The DSL will evaluate the strength and suitability of the current cyber security measures and consider improvements where necessary.

The DSL will ensure that the school's Safeguarding/ child protection policy adequately reflects its approach to online safety, including appropriate filtering and monitoring on school devices and school networks.

The DSL is responsible for taking any necessary action as per the Online Safety Incident reporting flowchart (Appendix 1).

They will arrange regular training and provide annual updates for all staff members about their responsibilities regarding online safety, filtering, and monitoring and acknowledge and understand the potential for serious child protection / safeguarding issues that arise from, but not limited to

- sharing of personal data
- accessing illegal / inappropriate materials
- exposure to inappropriate online content
- inappropriate contact with adults/strangers
- potential or actual incidents of grooming
- sexting
- cyber-bullying

In the event of a child protection or safeguarding incident pertaining to the above, the DSL will refer to appendix

Computing Lead / Team

The Computing Lead has the responsible for the teaching and learning of online safety across the whole school. The school has raised the profile of online safety and has expanded the computing curriculum to include a fourth strand of Digital Citizenship, the Education for a Connected World framework is used to support the teaching of Digital Citizenship and PHSE across all year groups.

The role of the Computing Lead/team includes:

· providing advice for staff and signpost relevant training and resources

· liaising with relevant outside agencies

· liaising with relevant technical support teams

· as needed to support DSL reviewing reports of Online Incidents (CPOMS)

· meeting regularly with Head teacher and relevant parties to discuss issues and subsequent actions.

· acting in response to issues identified

· communicating up-to-date Online Safety information to the wider school community

School Staff

It is essential that all staff:

· Receive annual appropriate safeguarding and child protection training, including online safety which, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
· Understand and acknowledge their responsibilities as outlined in this Policy.
· Have read, understood and signed the Staff Acceptable Use Policy
· Keep up to date with the Online Safety Policy as part of their CPD.
· Will not support or promote extremist organisations, messages, or individuals.
· Will not give a voice or opportunity to extremist visitors with extremist views.
· Will not browse, download, or send material that is considered offensive or of an extremist nature by the school.
· Have an up-to-date awareness of online matters pertinent to the pupils that they teach/have contact with
· Report concerns and log incidents. (CPOMS)
·Ensure that all digital communications with the School Community are on a professional level and only carried out using official school approved systems.
· Apply this Online Safety Policy to all aspects of the Curriculum.
·Share, discuss and ensure the pupils understand and acknowledge their responsibility to follow their age-appropriate Acceptable Use Agreements.
· Are good role models in their use of all digital technologies.
· Are vigilant in monitoring how pupils use digital technologies and access online content whilst in their care.

It is accepted that from time to time, for purposeful/appropriate educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable with clear reasons for the need

Technical support – Blue Orange

The school's technical infrastructure must be secure and actively reduces the risk of misuse or malicious attack.

To facilitate this, school has purchased support from Blue Orange.

The role includes:

· Follow the DFE digital and technology standards in schools
· provide a secure Wi-Fi system for both staff and guests with in your setting
· maintaining filtering and monitoring systems
· providing filtering and monitoring reports
· completing actions following concerns or checks to systems
· procure systems (with SLT &DSL)
· identify risk (with SLT &DSL)
· carry out reviews (with SLT &DSL)
· carry out checks (with SLT & DSL) ensuring that detected risks and/or misuse is reported to the Head teacher at school.
· ensuring that schools are informed of any changes to guidance or any planned maintenance.
· School technical systems will be managed and reviewed annually in ways that ensure that the school meets recommended technical requirements.
· All users will have clearly defined access rights to school technical systems and devices.
· All school network users will be assigned an individual username and password at the appropriate level of access needed for their role.
· ensuring internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation Child Abuse Image Content list (CAIC).
· Content lists are regularly updated, and internet use is logged and regularly monitored.
· There is a clear process in place to deal with requests for filtering changes.
· provide a platform where school should report any content accessible in school but deemed inappropriate.
· ensuring appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software (Appendix 2)

Pupils

The pupil's learning will progress through a broad, effective and relevant Online Safety curriculum.

A pupil's learning journey will be holistic in that it will include, but is not limited to their online reputation, online bullying and their health and wellbeing

In planning their online safety curriculum schools/academies may wish to refer to:

- DfE Teaching Online Safety in Schools
- Education for a Connected Word Framework
- SWGfL Project Evolve – online safety curriculum programme and resources

It is essential that all pupils should:

· Be able to recognise when something makes them feel uncomfortable (butterfly feeling) and know how to report it.
· Accept their responsibility to respond accordingly to any content they consider as inappropriate.
· Understand the importance of being a responsible digital citizen and realise that the school's Online Safety Policy applies to their actions both in and out of school.
· Know that school will act in response to any breach of the Online Safety Policy

Furthermore, online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing/PSHE/other lessons and should be regularly revisited/revised
- Key online safety messages should be reinforced through Teaching and Learning opportunities at their individual level.
- Pupils under 5 years old, will have limited screen time during school hours and will be co-viewing to support child development (questioning, understanding, routines).
- Pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils should be helped to understand the need for the child acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school/academy.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result

in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Parents / Carers / Responsible adults

Parents play an essential role in the education of their pupils and in the monitoring / regulation of the pupils's on-line usage. Due to the ever-evolving Digital World, adults can sometimes be unsure of how to respond to online risks and issues. They may also underestimate how often pupils encounter potentially harmful and inappropriate online material.

Therefore, it is essential that all adults should:

· Promote safe and responsible online practice and must support the school by adhering to the school's Safeguarding and Online Safety Policy in relation to digital and video images taken whilst on school premises or at school events.

· Understand, acknowledge that their child adheres to school procedure relating to their use of personal devices whilst on school grounds.

· To support the school community, school will provide information and awareness through, but not limited to:

· Letters, newsletters, website links, publications, external agencies

· Parents / Carer workshops

· High profile events / campaigns e.g. Safer Internet Day

Visitors entering school

It is essential that school apprise visitors of all relevant policies pertaining to their visit and contact with pupils.

Strategies for Teaching

- Online safety and AI education embedded in the curriculum (Computing, PSHE, RSHE, etc.) in age-appropriate and SEND appropriate formats.
- Regular training for staff (including governors) on online safety, AI risks, filtering & monitoring, SEND risk factors.
- Engage parents and carers: information, workshops or materials to help them understand online risks & safe use of AI tools at home.

Teaching styles will be adapted to allow pupils to observe, explore and discover, and so enhance the developmental process. No single style of teaching will suit all activities. Teaching will include:-

- Differentiated approaches to match age, ability, attainments, interests and experiences of the pupils.
- Appropriate content being selected.
- Pupils being encouraged to use their abilities to problem solve, gather information and acquire new skills.
- Social interaction and co-operation being fostered and reinforced through group teaching sessions.
- Teaching the class as a whole on some occasions.
- Pupils working individually sometimes.
- Pupils receiving one to one guidance when necessary.
- Pupils being offered challenges through the careful analysis of previous attainment and well-matched tasks and activities.
- Through organisation of teaching and learning environment, pupils will be given opportunity to generalise their learning in a variety of situations and contexts
- Development of a high-quality learning environment including displays, learning walls, book corners and outside areas etc.

Strategies for Learning

Effective Learning will take place via :-

- Pupils will take an active part in lessons.
- Pupils and teachers will have a sense of purpose.
- All staff will have positive expectations of pupils.
- Good use will be made of the opportunities to consolidate skills and use will be made of the knowledge that pupils have acquired.
- Pupils will be encouraged to think and communicate about their learning.
- Pupils will be encouraged to develop self-control.
- Independent working will be encouraged wherever possible.
- Pupils being given opportunities to work alone, in pairs, in groups and as part of a team.

Education – The Wider Community

The school will provide opportunities for local community groups/members of the community to gain from the schools/academy's online safety knowledge and experience. This may be offered through the following:

• Providing family learning courses in use of new digital technologies, digital literacy and online safety

• Online safety messages targeted towards grandparents and other relatives as well as parents.

• The school website will provide online safety information for the wider community

• Sharing their online safety expertise/good practice with other local schools

• Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision (possibly supporting the group in the use of Online Compass, an online safety self-review tool for groups such as these - www.onlinecompass.org.uk

Corrupting or destroying the data of other users

Below is a list of statements that would be considered as corrupting or destroying the data of other users and therefore is seen as a breach of this policy.

- Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
- Careless use of personal data e.g. holding or transferring data in an insecure manner
- Deliberate actions to breach data protection or network security rules
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with pupils
- Actions which could compromise the staff member's professional standing
- Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school/academy
- Using proxy sites or other means to subvert the school's/academy's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Breaching copyright or licensing regulations

Continued infringements of the above, following previous warnings or sanctions could result in further action being taken.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school/academy and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school/academy context, either because of the age of the users or the nature of those activities. Thus Ladywood has a strict filtering and monitoring policy in place (See technical Security document)

Use of AI in School

- **Approval and vetting**: Any AI / generative AI tool must be evaluated for safety, data protection, bias, privacy before use.
- **Product safety expectations**: Follow DfE guidance (product safety expectations for generative AI). EdTech Innovation Hub
- **Usage boundaries**:
    - Pupils use AI tools only under supervision / in structured settings.
    - Staff must not input sensitive personal data (staff or pupils) into AI tools which do not have confirmed data protection/security assurances.
    - AI must not replace human professional judgement or oversight.
- **Ethical considerations**: Address issues of bias, fairness, misinformation, hallucination, deepfake content, possibility of misuse (bullying, fostering false beliefs).
- **Curriculum & Digital Literacy**: Teach pupils about what AI is; its benefits and risks; how to evaluate AI-generated content; critical thinking about sources; safely sharing content online.
- **Incident response**: Clear procedures for when things go wrong (e.g. misuse of AI, harmful AI content, data breach via AI) including record keeping, reporting, parental communication, external agencies if required.

Safeguarding/Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.
If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (Appendix 1) for responding to online safety incidents and report immediately to the police.

In the event of a Safeguarding infringement or suspicion, appendix 1 must be followed with consideration of the following:

· Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

· Conduct the procedure using a computer that will not be used by pupils and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

· It is important to ensure that the relevant staff should have appropriate internet access to conduct the investigation, but also that the sites and content visited are closely monitored and recorded (to provide further protection)

· Record any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots

of the content on the machine being used for investigation. These may be printed and signed (except in the case of images of child sexual abuse – see below)

· If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include incidents of 'grooming'

Behaviour the sending of obscene materials to a child adult material which potentially breaches the Obscene Publications Act criminally racist material other criminal conduct, activity or materials. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the relevant group for evidence and reference purposes.

Data Protection

Personal and sensitive data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Schools are audited regularly regarding how they handle their data, for further information please refer to school Data Protection Policy.

- Comply with UK GDPR, Data Protection Act and school's data protection policies.
- Personal data must be protected, especially when using online tools and AI.
- Ensure AI vendors/third-party tools have appropriate data protection agreements, security assurances.
- Secure management of devices, access, passwords.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm: (select/delete as appropriate)

• When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

• Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/social media/local press (may be covered as part of the AUA signed by parents or carers at the start of the year - see parents/carers acceptable use agreement in the appendix)

• In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their pupils at school/academy events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
• Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school/academy equipment; the personal equipment of staff should not be used for such purposes.
• Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school/academy into disrepute.
• Pupils must not take, use, share, publish or distribute images of others without their permission
• Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
• Pupils'/Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
• Pupil's/Pupil's work can only be published with the permission of the pupils/pupil and parents or carers.

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.
All users should understand that the primary purpose of the use mobile/personal devices in a school context is educational. More information can be found in the staff code of conduct policy under the heading mobile phones and within the technical security policy.

Communications

When using communication technologies the school considers the following as good practice:

· The Office 365 school email service is safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school.

· When accessing emails out of the schools setting, staff will only be able to access their schools' emails using Microsoft Multifactor Authentication app.

· Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel

uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

· Any digital communication between staff and pupils or parents / carers (email, chat) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.

· Pupils should be taught about online issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Social Media



The school's use of social media is to promote the ethos of the school. It is the responsibility of all staff to ensure that the content they upload is for professional purposes only, be compliant with the school policies and protect the identity of pupils. Please also refer to Ladywood's Social Media Policy.

Assessment, Recording & Reporting

The procedure for assessment, recording & reporting will be in line with school practice for the whole curriculum.

Resources will be purchased by the subject manager on an annual basis. Staff are encouraged to notify the subject manager of their needs.

All staff must report any online safety or AI-related concerns to the DSL immediately.

- Keep detailed records of incidents (what, when, who, what harm).
- In cases of serious harm (e.g. child sexual abuse material, grooming, deep-fake pornography, etc.), follow safeguarding procedures including reporting to external agencies (e.g. police, CEOP).
- Support pupils involved (including SEND pupils) with pastoral care, counselling, restorative approach where appropriate.

Ethnicity & Equal Opportunities

Our policy is designed to be culturally appropriate and inclusive of all pupils. We will aim to avoid any form of racism, sexism and stereotyping.

Community Links

The emphasis is upon learning within the home, school and community. Pupils will be given the opportunity to transfer knowledge, skills, attitudes and concepts that they have learnt to other situations. Some pupils are offered time learning in other settings, e.g. mainstream schools, museums, nurseries. Social inclusion is encouraged wherever possible. Opportunities are created for the pupils to develop awareness of other cultures.

Partnership with Parents

At Ladywood, we strive to build and maintain an atmosphere of mutual respect and dialogue in which the needs of pupils are paramount. We believe firmly in the need for involvement of parents and carers in the education of their pupils at Ladywood.

Monitoring the Policy

The Governing Body is responsible for ensuring that the school complies with legislation, and that this policy and its related procedures and strategies are implemented

- Policy to be reviewed at least annually (or sooner if legal/technological change).

- The DSL reports to governors/proprietors on online safety, AI tool usage, risk assessments, filtering & monitoring effectiveness, incidents.
- Include in school self-evaluation and safeguarding audits.
- Governors should ensure that resourcing is sufficient (training, technical, staffing) to implement policy.

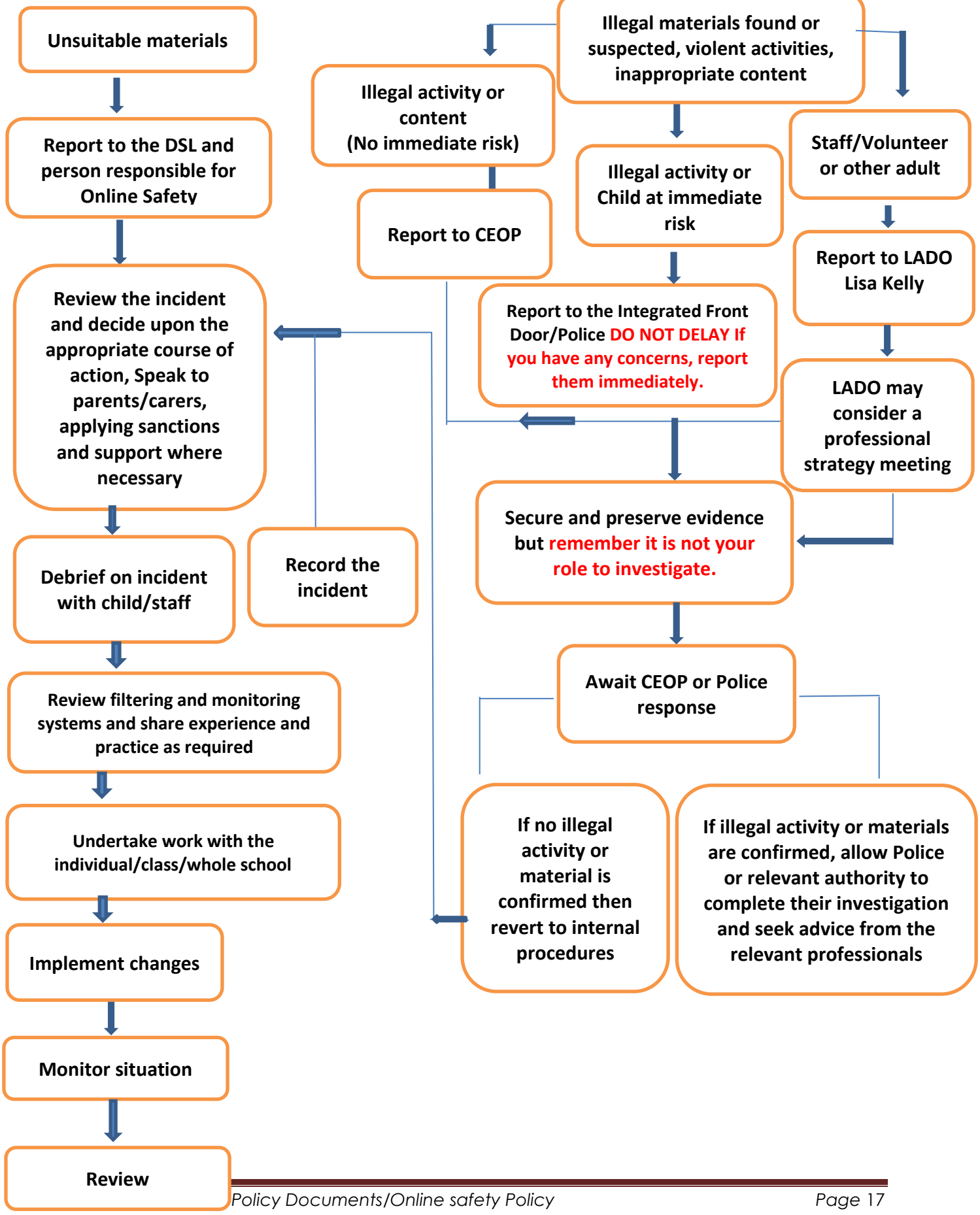
Dissemination of the Policy

Head teacher, governors, all staff members and health professionals will have access to this policy. Copies are available in school for parents on request.

Appendix 1

Online Safety Incident Reporting

Safeguarding in Education Team
Bolton Safeguarding Children



Support for Blue Orange

Next steps

- Consider if an individual safety plan is required
- Consider opening an early help assessment
- Ensure that data inputting procedures are in place and that data is shared with relevant governance

Appendix 2

Bolton Schools ICT
Putting Schools First

TECHNOLOGY STANDARDS

FOR PRIMARY SCHOOLS 2023

CONTENTS

Timetable for meeting Technology standards

Executive summary

Fundamental Technical Principles

DFE Standards

Broadband Internet Standards

Network Switching Standards

Network Cabling Standards

Wireless Network Standards

Cyber Security Standards

Filtering and Monitoring Standards

Cloud Solution Standards

Servers and Storage Standards

Timetable for meeting Technology Standards

Technology Standard	NOW	ASAP	AT NEXT UPDATE
Broadband Internet Standards			
Schools and colleges should use a full fibre connection for their broadband service			
Schools and colleges should have a backup broadband connection to ensure resilience and maintain continuity of service			
Schools and colleges should have appropriate IT security and safeguarding systems in place, under both child and data protection legislation			
Network Switching Standards			
The network switches should provide fast, reliable and secure connections to all users both wired and wireless			
Have a platform that can centrally manage the network switching infrastructure			
The network switches should have security features to protect users and data from unauthorised access			
Core network switches should be connected to at least one UPS to reduce the impact of outages			
Network Cabling Standards			

Copper cabling should be Category 6A (Cat 6A)			
Optical fibre cabling should be a minimum 16 core multi-mode OM4			
New cabling should be installed and tested in line with the manufacturer's guidance, warranty terms, and conditions			
Wireless Network Standards			
Use the latest wireless network standard approved by the Wi-Fi Alliance			
Have a fully functional signal from your wireless network throughout the school or college buildings and externally where required			
Have a solution that can centrally manage the wireless network			
Install security features to stop unauthorised access			
Cyber Security Standards			
Protect all devices on every network with a properly configured boundary or software firewall			
Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date			
Accounts should only have the access they require to perform their role and should be authenticated to access data and services			
You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication			
You should use anti-malware software to protect all devices in the network, including cloud-based networks			
An administrator should check the security of all applications downloaded onto a network			
All online devices and software must be licensed for use and should be patched with the latest security updates			
You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site			
Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack			
Serious cyber-attacks should be reported			
You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation			
Train all staff with access to school IT networks in the basics of cyber security		Within 12 months	
Filtering and Monitoring Standards			
You should identify and assign roles and responsibilities to manage your filtering and monitoring systems			
You should review your filtering and monitoring provision at least annually			
Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning			
You should have effective monitoring strategies that meet the safeguarding needs of your school or college			

Cloud Solution Standards			
Use cloud solutions as an alternative to locally-hosted systems, including servers			
Cloud solutions must follow data protection legislation			
Cloud solutions should use ID and access management tools			
Cloud solutions should work on a range of devices and be available when needed			
Make sure that appropriate data backup provision is in place			
Servers and Storage Standards			
All servers and related storage platforms should continue to work if any single component or service fails			
Servers and related storage platforms must be secure and follow data protection legislation			
All servers and related storage platforms should be energy-efficient and set up to reduce power consumption, while still meeting user needs			
All server and related storage platforms should be kept and used in an appropriate physical environment			

This document focuses on the guidance published by DFE on meeting digital and technology standards in school and colleagues found at: Government technology standards and guidance - GOV.UK (www.gov.uk) This summary is designed for school leaders to introduce the concept of what, at a high level, is required to take place. The document then goes on to the technical details, referencing the DFE technical standard document where they exist and providing additional detail when they do not so that a holistic solution is referenced.

Broadband Internet Standards

The Bolton Schools ICT broadband SLA provided connection exceeds the speed required in this standard.

The connection is protected by a Sophos Unified Threat Management device configured at the 'edge' of the network. This is maintained and monitored by SICT. This provides Firewall and Web Filtering. From September 2023 the monitoring is provided by a product called FastVue which works alongside the web filter to provide reports and alerts.

BSICT are currently undergoing a review of this service, and whilst it is likely the product may change, this will be at least an equal match to the current solution in place, with some improvements due to advances in technology and services offered by supplies. For example, a backup connection will be provided in the next round of updates to the broadband connections in schools.

Network Switching Standards

All the switches currently available and those supplied in the last 5 years from Bolton Schools ICT meet the following requirements:

1. To provide 1Gbps connectivity to end user devices.
2. Centrally managed and monitored.

Our default switch configuration securely separates the network into 3 parts, internal secure network, external network, guest wireless network, and VOIP Telephony networks. Using VLANs prevents these separate networks from accessing each other.

Bolton Schools ICT can quote for new switches which meet the requirement for higher speeds to servers and infrastructure devices on request.

It is important to note that the ability of the switch to deliver this higher speed is dependent on the specification and quality of physical cabling, and this may also need to be upgraded to meet the separate DfE cabling standard when new networking equipment is installed.

A UPS can be provided to provide power backup to your core switches as necessary, this is often of limited benefit to primary schools.

Bolton Schools ICT can survey and audit your network switches and provide recommendations to help you meet standards if not already. This can present a significant cost to school to meet, so a cost-benefit analysis would need to be carried out which we can advise on potential benefits.

Switch: Meeting digital and technology standards in schools and colleges - Network switching standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Network Cabling Standards

Having your school fully rewired with new cabling is a major expense.
Most schools will have Category 5E or 6 cabling. This is suitable to provide 1Gbps connectivity to the desktop as required in the switching standards.
Category 6A cabling is capable of supporting 10Gbps which is generally only used for infrastructure links.

In order to meet the network cabling standards, it is highly likely that you will need to upgrade all your network cabling. Only new build schools or those with recently installed cabling are likely to meet this standard.
Bolton Schools ICT can carry out an initial basic survey to advise and assist with a cost-benefit analysis, but for a full quote or for work to be carried out you will need to engage with a cabling contractor. Bolton Schools ICT can assist you with providing the specification to the contractor and engaging in technical discussions.

Cabling: Meeting digital and technology standards in schools and colleges - Network cabling standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Wireless Network Standards

The newest wireless access points available from Bolton Schools ICT meet the technical requirements of this standard. Bolton Schools ICT offer a wireless survey as part of quoting for the network and can arrange coverage across school as necessary.
New installs will all have a segregated guest wireless network as standard, and older installs are being upgraded on a rolling basis where possible.

Schools are not required to meet this standard until your existing setup is replaced when it is either underperforming or unsupported. However, you will likely need to consider upgrading your network cabling as well at the same time, as installing a new wireless network triggers the requirement to meet the network cabling standards which present a considerable expense to school.

Cyber Security Standards

All schools utilising Bolton Schools ICT Broadband SLA are provided with an industry leading edge firewall and filtering device. They also get Sophos anti-virus as part of this SLA. This

meets all the relevant requirements and is monitored and maintained as part of the SLA agreement.
Bolton Schools ICT will maintain network accounts based on requests from school and will keep a log of requests via our calls system. It is the responsibility of each school to ensure that they keep these accounts up to date and request account deactivation when staff leave. Bolton SICT can advise on how to maintain the security of your network drives so that data can only be accessed by those with permission.
Bolton Schools ICT recommend that schools use the "Cyber Security Training for School Staff" materials from the NCSC. Schools must ensure that they deliver this training every year. It is recommended that a log is kept of this training and staff completing the training download their certificate. This training should also be offered to school governors with the expectation that at least one governor completes the training every year. Any new members of staff must complete this Cyber security training as part of their induction into the school.
As part of our service into schools, Bolton Schools ICT will review the suitability, quality and effectiveness of these measures every year.

Filtering and Monitoring Standards

Schools utilising the Bolton Schools ICT broadband SLA meet this standard. Over the summer we have purchased and deployed a new monitoring system to meet the requirements for monitoring and alerts. Our existing web filter meets the filtering requirements.

Cloud Solution Standards

Schools ICT manage a Bolton-wide tenancy on Microsoft 365 for all schools utilising this service. This includes email, Teams and some schools use OneDrive/SharePoint as well. This is a hybrid solution, as schools also have a local server.
Data in our Microsoft 365 tenancy is stored within the UK or EU.
The cloud data transfer is protected behind HTTPS encryption. Logon requires multi-factor authentication when accessed outside the school secure network.
There is currently no additional backup in Microsoft 365 beyond that provided by Microsoft where deleted items can be recovered within around 30 days. Data which needs to be properly backed up must be kept on the school server.
We are investigating options for schools who wish to move more of their services into the cloud and will provide information in due course, or if you would like more information, please contact us.

Servers and Storage Standards

As part of the SLA, SICT will monitor your server for failure using Dell's OpenManage software, and Microsoft Systems Centre Operations Manager. If a failure is detected a technician will investigate and a quote will be sent to schools for replacement hardware if not covered by warranty.
All new servers provided after September 2023 will come with multiple power supplies for redundancy, this will present an increased cost.
All servers provided by Bolton Schools ICT come with 3 year's onsite warranty and maintenance from date of installation.

Bolton Schools ICT will keep your servers up to date and patched.
Your server should be kept in a secure location in school that is not accessible to unauthorised persons. This can either be a locked cupboard, or a secure purpose-built room. SICT can assist with moving your server if this is necessary to meet this requirement. You may need to have extra power and data points fitted, and the room or cupboard must not be used for other purposes.

Appendix 4

Details of ALL Online incidents to be recorded by the staff within your School, this incident log will be monitored weekly by the DSL .

Date & time	Name of child or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons

Definitions (Key Terms)

- **Online harms**: content or contact that may cause harm including pornography, radicalisation, grooming, self-harm but now explicitly includes misinformation, disinformation, conspiracy theories. EdTech Innovation Hub+2Education Experts+2
- **Generative Artificial Intelligence (AI)**: tools that can create new content (text, images, video, voice, etc.).
- **Filtering and Monitoring**: technical systems and policies to control access to harmful content and to observe use of devices/systems for safeguarding.
- **SEND Vulnerabilities**: pupils with SEND may face additional risks (e.g. less able to recognise online harm, more dependent on adults, or more trusting of digital personas).